REMARKS

Claims 1-37 and 39-41 are currently pending in the subject application and are presently under consideration. Claims 1, 28 and 34 have been amended as shown on pp. 2 and 5, respectively, of the Reply. In addition, claim 5 is cancelled with this Reply.

The Examiner is thanked for courtesies extended in a telephonic interview on Friday May 2, 2008. Discussed during the interview were the merits of filing a 131 Declaration with respect to several of the above claims, suitable amendments to overcome the 35 U.S.C. §101 rejection, and discussion of differences in the recited subject matter of claims 12, 13, 18, 19, and 21 with respect to Rayes *et al.* Furthermore, addition of a new claim was proposed during the interview.

Due to logistic reasons regarding applicants, the 131 Declaration is not being pursued at this time. Thus, amendments have been made to independent claims 1, 28 and 34 to traverse the cited reference and advance prosecution. These amendments include the significant aspects of the new claim proposed during the interview, so this claim does not appear separately, but is incorporated into claim 1 as amended. In addition, claims 1, 28 and 34 are amended to recite systems embodied on a computer-readable storage medium, to overcome the 35 U.S.C. §101 rejection.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-37 Under 35 U.S.C. §101

Claims 1-37 stand rejected under 35 U.S.C. §101 because the Examiner contends the claimed invention is directed to non-statutory subject matter. Independent claims 1, 28, and 34 have been amended to address the Examiner's concerns with regard to this rejection. It is therefore respectfully requested that this rejection be withdrawn.

II. Rejection of Claims 1-37 and 39-41 Under 35 U.S.C. §102(e)

Claims 1-37 and 39-41 stand rejected under 35 U.S.C. §102(e) as being anticipated by Rayes *et al.* (U.S.2005/0086502 A1). Withdrawal of this rejection is requested for at least the following reasons:

A. Rayes, *et al.* does not teach or suggest each and every feature set forth in the

subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject claims relate to a system and method for gathering and aggregating data relating to the health, performance, and utilization of one or more networked systems, and utilizing the aggregated data to generate outputs relating to the state of the one or more networked systems. The outputs can be used to notify a user (*e.g.* a system administrator) of potential problems detected on the system, generate reports based on the data, and provide automatic control on aspects of the networked system in response to the detected system state. The output can also be used to automatically limit aggregate utilization of one or more aspects of the system. For example, the system can monitor and limit overall bandwidth usage, e-mailing faxing, or Internet usage. In particular, amended independent claim 1 recites, *an aggregator that analyzes an aggregate of at least a subset of the system data and generates an output corresponding to a state of a subset of the plurality of system components,* ***the output utilized to automatically limit aggregate utilization of at least one aspect of the networked system according to a defined limit on overall utilization.***

Rayes, *et al.* does not disclose these aspects of the subject claims. Rayes, *et al.* relates to a security management system that can monitor a system's network health and security alerts, and use this information to take corrective measures against malicious activity by a system user. However, these corrective measures are not aimed at limiting *aggregate utilization* of system resources. Rather, the corrective measures are targeted at *individual users* according to calculated user risk levels associated with each user (see at least paragraphs [0038], [0057], [0063], [0080], and [0086]). Moreover, curtailment of a user's activity on the system is not driven by a *defined limit on an overall utilization of a system resource*, but rather is based on an alert state for the system combined with the aforementioned user risk associated with the user.

The subject claims also disclose that the aggregated data can be used to detect other undesired system states and to automatically effectuate corrective responses. This can include

providing software updates to a system component when a potential problem or software bug is discovered. Moreover, when an immediate fix for the error state is not available, alerts generated by the error state can be masked to prevent false indications to a system or administrator. Specifically, amended independent claim 28 recites, *utilizing the output to provide an automatic software update to at least one system component to mitigate a detected error state; and masking alerts associated with the error state when a software update is not available.* Rayes, *et al.* does not teach or suggest automatically providing software updates in response to a detected error state. Although, as the Examiner indicates, Rayes, *et al.* describes a hardware environment on which the cited security system can be run that provides for downloading the security application code from the Internet, it is noted that this is merely intended to illustrate that the security system code itself can be delivered to a computer *via* the Internet. This disclosure alone in no way suggests automatically providing software updates to a system component *in response to a detected error state*. Indeed, such updates are nowhere disclosed in the cited reference. Nor does Rayes, *et al.* teach that alerts associated with an error state can be masked when such an update is not available.

In addition to the features discussed above, the subject claims also disclose that individual utilization of system resources can be limited according to a user-defined utilization priority. This feature allows a first user's utilization of a system resource to automatically be made subservient to a second user's utilization of the same resource if the second user has a higher utilization priority. In particular, amended independent claim 34 recites, *means for prioritizing utilization of at least one resource on the networked system; and means for* ***automatically curtailing utilization of a resource by a first user of the networked system when a second user with a higher utilization priority requires the same resource.*** The Examiner cites a section of Rayes, *et al.* that discloses disabling a user's network access if the user is determined to have a high risk level. However, this user rejection is not initiated by a higher-priority user's attempts to access to a shared resource, as recited in amended independent claim 34. Rather, the user's high risk level triggers the rejection, independently of another user's attempts to access a same resource. It therefore cannot be said that the risk-based user curtailment taught by Rayes, *et al.* cannot be said to read on the utilization priority features of amended independent claim 34.

Furthermore, claim 19 recites, *the output utilized to provide* ***automatic software updates*** *to at least one system component on the networked system in response to the state of the subset of*

the plurality of system components, and as already noted, Rayes, *et al.* does not disclose such automatic software updates.

B Each and every element of at least dependent claims 12, 13, 18, 19, and 21 is not taught, disclosed or suggested by Rayes *et al.*

Claim 12 recites the elements of independent claim 1 in conjunction with the output comprising hidden information obtained *via* data mining of aggregated system data. Rayes *et al.* discloses, in general, a mechanism for monitoring a health state of a network, user threat level and/or performance of system components to determine whether to restrict user access to the system. Rayes *et al.* does disclose that data pertaining to these monitored aspects can be stored in a common database (*e.g.*, at paragraph 60), but does not disclose employing data mining to obtain hidden information from aggregated system data. Data mining to extract hidden information available within an aggregate of data, such as historical trends, current network activity and/or projected future activity, can provide richer, more meaningful information of system health and user threat. Rayes *et al.* simply provides a baseline measurement of system health compared with user threat level and/or component performance. It doesn't employ data mining to extract hidden trends and other information from aggregated data, as described above. Thus, each and every aspect of claim 12, and claim 13 which depends there from, is not taught, disclosed or suggested by the cited reference.

Regarding claim 18, Rayes *et al.* also does not recite output utilized to detect faulty errors in a networked system. Rayes *et al.* discloses determining a risk level based on several factors, but has no mechanism to determine whether a detected error is proper or not. Thus, Rayes *et al.* exposes a system to potential false errors, where claim 18 provides a mechanism to mitigate such events. With regard to claim 19, Rayes *et al.* does not teach, disclose or suggest the output utilized to provide automatic software updates to at least one system component on the networked system in response to the state of the subset of the plurality of system components. Rather, Rayes *et al.* is limited to limiting or blocking user access to a system in response to a system health, performance or user threat level. With respect to claim 21, Rayes *et al.* is silent with respect to the system control parameter comprises at least one of a load shed command or a load balancing command, and thus does not teach, disclose or suggest this claimed element.

C. Claim 5 is cancelled with this Reply. Accordingly, because the cited reference does not teach, disclose or suggest each and every aspect of claims 1-4, 6-37 and 39-41, and because claim 5 is cancelled with this Reply, withdrawal of the rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP503USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731